IoT-Sicherheit: Digitale Zertifikate zum Schutz vernetzter Geräte

Wie Sie mit der xc-Produktfamilie Ihre IoT/OT-Landschaften sicherer machen

Rasantes Wachstum

Laut statista.com wird sich die Anzahl der IoT-Geräte von 2023 bis zum Jahr **2030** fast verdoppeln und auf rund **29,5 Milliarden Geräte** ansteigen. Diese gigantische Zahl und das rasante Wachstum zeigen, dass die Absicherung von IoT-Geräten eine zentrale Herausforderung der Cybersicherheit darstellt.

Denn die verschiedenen Geräte und Devices sind meist miteinander zu ganzen IoT-Systemen vernetzt. Je umfangreicher das System, desto zahlreicher sind die Angriffsvektoren und desto gravierender die Folgen eines gelungenen Cyberangriffs. Hat es ein Angreifer erst einmal geschafft, in ein Netz von IoT-Systemen einzudringen, kann er **Prozesse lahmlegen** oder sogar **Komponenten zerstören** und somit großen Schaden anrichten.

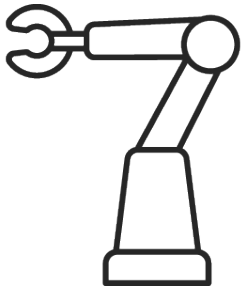
Die Angriffsziele sind vielfältig. Waren früher vor allem Smart Home Geräte betroffen, sind heute vor allem Business-Systeme für Cyberkriminelle interessant.

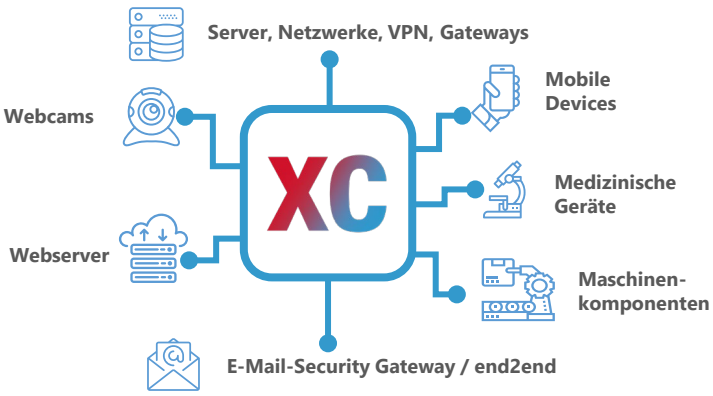
Gefahr für jegliche technischen Anlagen

In den letzten Jahren waren Nachrichten über erfolgreiche Cyberattacken vermehrt in der Presse. Neben z.B. Automobilzulieferern waren sogar Krankenhäuser unter den Opfern.

Gefährdete Umgebungen können sein

- Industrieanlagen
- Shopfloor-Systeme
- Fertigungs- und Produktionssteuerung
- Verpackungsmaschinen
- Gebäudetechnik und Aufzugssteuerungen
- Alarmanlagen
- Roboter
- Bankautomaten
- Und viele weitere





Risiken entstehen vor allem, wenn

- die Kommunikation zwischen den Komponenten nicht abgesichert ist, d.h. die Geräte unverschlüsselt miteinander kommunizieren
- unsichere Schlüssel und Zertifikate für die Verschlüsselung verwendet werden
- Schlüssel und Zertifikate ohne Ablaufdatum eingesetzt werden
- Devices und Geräte nicht eindeutig identifizierbar sind.

Haben es Cyberkriminelle geschafft, sich in ein unzureichend geschütztes IoT-Gerät zu hacken, können sie von dort aus das ganze System übernehmen. In diesem Fall drohen

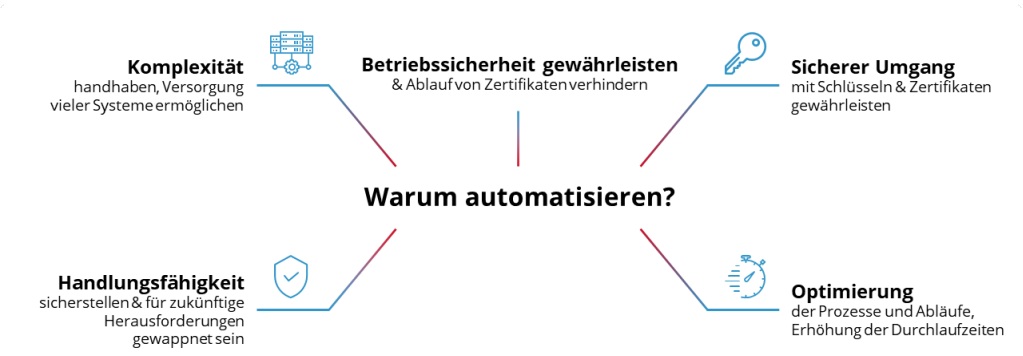
- Datendiebstahl
- Datenmanipulation
- Ausfall von Gebäudetechnik (Mitarbeiter Gebäude nicht mehr betreten, Aufzüge fahren nicht mehr)
- Störung oder Stilllegung von Produktions- und Steuerungsanlagen

Die Wiederherstellung eines sicheren und funktionierenden Netzwerks ist langwierig und aufwändig, so dass mit **Lieferverzögerungen** oder gar **Produktionsausfall** zu rechnen ist.

Möchten Sie mehr erfahren oder die Lösung anhand einer Demo kennenlernen? Wir beraten Sie gerne.

Kontakt EU essendi it GmbH, Dolanallee 19, DE-74523 Schwäbisch Hall +49 791 943 07 011 info@essendi.de essendi.de
Kontakt international essendi it AG, Bahnhofplatz 1, CH-6460 Altdorf, UR +41 41 874 27 30 info@essendi.ch essendi.ch

Um die Sicherheit von IoT/OT-Systemen zu gewährleisten, besteht Handlungsbedarf an mehreren Stellen.



Effektive Schutzmaßnahmen

Es ist wichtig, die eigenen Schwächen zu erkennen. Nur dann kann man effektive Schutzmaßnahmen ergreifen. Ein umfassender **Überblick über den Status der Geräte**, sowie deren **Überwachung** und **Verwaltung** sind also notwendig. Dann können potenzielle Bedrohungen rechtzeitig erkannt und Gegenmaßnahmen ergriffen werden.

Dies ist besonders entscheidend, da im Zuge von **Industrial IoT (IIoT)** bzw. **Industrie 4.0** die Bereiche der Betriebstechnik und IT immer mehr Berührungspunkte haben und verschmelzen. Schwachstellen sind nicht nur eine Gefahr für Industrieunternehmen, sondern auch für KRITIS-Unternehmen wie Strom- und Energieversorger, Wasserwirtschaft, Lebensmittelindustrie und sogar Banken.

Sichere IoT-Landschaften

Neben dem regelmäßigen Einspielen von Sicherheitspatches und Updates machen folgende Maßnahmen die **Kommunikation zwischen IoT-Geräten** sicherer:

- Verschlüsselter Datenverkehr zwischen allen Komponenten (TLS/SSL)
- Management der privaten Schlüssel der Komponenten mittels Zertifikate
- Sichere Schlüssel und Zertifikate mit regelmäßigem Ablaufdatum und regelmäßiger Erneuerung
- Inventory-Management für die Devices
- Eine digitale Identität für jedes Gerät
- Berechtigungsmanagement für die Devices
- Multifaktor-Authentifikation
- Monitoring und Überwachung zur Früherkennung von Angriffen

Die essendi xc-Produktfamilie als Brücke zwischen IoT/OT und IT

Sicherheitsvorkehrungen erfordern hohe Aufwände für die IT-Systemadministration, die bei der Vielzahl und Heterogenität der Geräte manuell nicht zu stemmen sind.

Die Produktfamilie essendi xc bietet bewährte Lösungen, um IoT-Landschaften sicherer zu machen und gleichzeitig die IT-Administratoren von Routineaufgaben im Zertifikatsbereich zu entlasten.

So findet **essendi cd** Zertifikate aller Ausprägungen aus verschiedensten Quellen im gesamten Rechenzentrum und kann sie in das zentrale Repository von essendi xc integrieren.

essendi xc übernimmt dann das Management der Zertifikate über deren gesamten Lebenszyklus hinweg. Mit essendi xc werden alle Abläufe vollständig automatisiert:

- Zertifikate anfordern, ausstellen und im Zielsystem installieren
- Alerting über bevorstehende Zertifikatsabläufe
- Zertifikate erneuern, wenn erforderlich
- Alle Komponenten und Devices werden eindeutig identifiziert

Das Schlüsselmaterial ist unter zentraler Kontrolle. Bei Bedarf (und wenn die Geräte es unterstützen) können Schlüssel direkt auf den IOT-Geräten erzeugt werden. Auch kryptografische Operationen - wie das Signieren des CSR, etc. - sind möglich

Das hohe Maß an Automatisierung entlastet die IT-Administratoren, bzw. macht IoT-Security erst möglich.

Möchten Sie mehr erfahren oder die Lösung anhand einer Demo kennenlernen? Wir beraten Sie gerne.

Kontakt EU essendi it GmbH, Dolanallee 19, DE-74523 Schwäbisch Hall +49 791 943 07 011 info@essendi.de essendi.de
Kontakt international essendi it AG, Bahnhofplatz 1, CH-6460 Altdorf, UR +41 41 874 27 30 info@essendi.ch essendi.ch